REDACTED VERSION OF DOCUMENT TO BE SEALED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

In re Flagstar December 2021 Data Security Incident Litigation	Case No. 4:22-cv-11385 Hon. Shalina D. Kumar

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO FLAGSTAR'S MOTION TO DISMISS

REDACTED VERSION OF DOCUMENT TO BE SEALED

TABLE OF CONTENTS

REDACTED VERSION OF DOCUMENT TO BE SEALED

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

CONCISE STATEMENT OF THE ISSUES PRESENTED

1. Whether Plaintiffs have Article III standing to bring their claims.

2. Whether Plaintiffs sufficiently alleged a negligence claim based on Flagstar's failure to adequately secure their sensitive personal information.

3. Whether Plaintiffs sufficiently alleged a breach of confidence based on Flagstar's failure to prevent the disclosure of their sensitive personal information.

4. Whether Plaintiffs sufficiently alleged invasion of privacy based on Flagstar's intentional failure to address known vulnerabilities in its data systems and the resulting public disclosure of their sensitive personal information.

5. Whether Plaintiffs sufficiently alleged a breach of express contract claim.

6. Whether Plaintiffs sufficiently alleged a breach of implied contract claim.

7. Whether Plaintiffs sufficiently alleged that Flagstar was unjustly enriched by the acceptance of monies and fees for its services without providing adequate security for Plaintiffs' sensitive personal information.

8. Whether Plaintiffs sufficiently alleged a declaratory judgment claim.

9. Whether Plaintiffs stated a claim for violation of the California Customer Records Act and the Washington Data Breach Disclosure Law.

10. Whether Plaintiffs stated claims for unfair or deceptive conduct under state statutes in California, Colorado, Indiana, Michigan, and Washington.

11. Whether Plaintiffs sufficiently alleged a violation of the California Consumer Privacy Act.

CONTROLLING OR MOST APPROPRIATE AUTHORITIES

Authority supporting Plaintiffs' Article III standing:

Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016)

In re Blackbaud, Inc., Customer Data Breach Litig., 2021 WL 2718439 (D.S.C. July 1, 2021)

Authority supporting Plaintiffs' negligence claims:

In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020)

I*n re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295 (N.D. Ga. 2019)

Authority supporting Plaintiffs' breach of confidence claim:

McGuire v. Shubert, 722 A.2d 1087 (Pa. Super. Ct. 1998)

Milohnich v. First Nat. Bank of Miami Springs, 224 So. 2d 759 (Fla. Ct. App. 1969)

Authority supporting Plaintiffs' breach of privacy claim:

Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898 (S.D. Cal. 2020)

McKenzie v. Allconnect, Inc., 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019)

Authority supporting Plaintiffs' breach of contract claims:

Hummel v. Teijin Auto. Techs., Inc., 2023 WL 6149059 (E.D. Mich. Sept. 20, 2023)

Lochridge v. Quality Temp. Servs., Inc., 2023 WL 4303577 (E.D. Mich. June 30, 2023)

Authority supporting Plaintiffs' unjust enrichment claim:

In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020)

Authority supporting Plaintiffs' declaratory judgment claim:

In re: Home Depot, Inc. Customer Data Sec. Breach Litig., 2016 WL 2897520 (N.D. Ga. May 18, 2016)

Authority supporting Plaintiffs' California Customer Records Act and Washington Data Breach Disclosure Law claims:

Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898 (S.D. Cal. 2020)

In re Mednax Servs., Inc., Customer Data Sec. Breach Litig., 603 F. Supp. 3d 1183 (S.D. Fla. 2022)

Authority supporting Plaintiffs' claims for unfair or deceptive conduct under state statutes in California, Colorado, Indiana, Michigan, and Washington:

In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020)

In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 2019)

In re Experian Data Breach Litig., 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016)

Bray v. Gamestop Corp., 2018 WL 11226516 (D. Del. Mar. 16, 2018)

Williams v. Foremost Ins. Co. Grand Rapids Michigan, 2018 WL 1907523 (W.D. Wash. Apr. 23, 2018)

Authority supporting Plaintiffs' California Consumer Protection Act claim:

Morgan v. AT&T Wireless Servs., Inc., 177 Cal. App. 4th 1235 (2009)

REDACTED VERSION OF DOCUMENT TO BE SEALED

INTRODUCTION

Flagstar[1] is the second largest mortgage warehouse lender nationally. It collects vast troves of personal information from its customers and profits from that data through its own marketing efforts and by sharing sensitive customer information with third parties. Flagstar assures customers through its Privacy Statement that it is "committed to maintaining the security of the data you provide us," and promises "[t]o protect your personal information from unauthorized access and use" through "security measures that comply with federal law," including "computer safeguards and secured files[.]"[2] But for the second time in a single year, Flagstar failed to meet these obligations.

This case involves the second of these two back-to-back breaches. From November 2021 through December 2022, Flagstar suffered a data breach compromising the sensitive personally-identifiable information ("PII"), including full names and Social Security numbers, of over 1.5 million former and current Flagstar customers. Flagstar's conduct resulted in catastrophic outcomes for Flagstar's customers, who already sustained or face a serious risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Further,

[1] New York Community Bancorp., Inc. f/k/a/ Flagstar Bancorp, Inc. and Flagstar Bank, N.A., f/k/a Flagstar Bank, FSB (collectively, "Flagstar").
[2] Consolidated Class Action Complaint ("CAC"), ECF No. 52 PageID.544–656, ¶¶ 1, 26.

they did not receive the benefit of their bargain with Flagstar and the breach diminished the value of their PII.

Plaintiffs have standing under Article III: the data breach compromised highly sensitive personal information, Flagstar itself recognized that the breach puts Plaintiffs at substantial risks when it urges customers to monitor their accounts and offered them credit monitoring services; and it can be reasonably inferred that the concrete injuries Plaintiffs have already experienced are traceable to the breach. Flagstar's premature attack on the merits of Plaintiffs' injuries, disguised as a "factual attack" on standing, does not change this result: Flagstar has not disproven Plaintiffs' detailed allegations that their PII was misused by cyber criminals and that they are at a significantly increased risk of identity theft.

Flagstar's arguments for dismissal are unavailing. Plaintiffs sufficiently pled their common law and statutory claims. Flagstar harmed Plaintiffs when it breached its duty to adequately secure Plaintiffs' personal information. Flagstar promised to safeguard Plaintiffs' personal information, invaded Plaintiffs' privacy, breached their confidence by failing to do so, and reaped ill-gotten gain by profiting from Plaintiffs' information but failing to devote sufficient resources to secure it. That failure also constitutes an unfair practice under state consumer statutes, and Flagstar engaged in deceptive practices by misrepresenting and failing to disclose its inadequate data security. Flagstar's Motion to Dismiss should be denied.

STATEMENT OF FACTS

I. The Declaration Of Jennifer Charters.

The centerpiece of Flagstar's factual attack on standing is the declaration of Jennifer Charters, Flagstar's Chief Information Officer ("CIO"). But Ms. Charters did not prepare her declaration and does not know who did.[3] With the understanding that the information contained therein was "information from Flagstar," Ms. Charters signed it without making any revisions and after consulting virtually no documents.[4] Information security is not within Ms. Charters' purview,[5] and she has no relevant firsthand knowledge of the matters discussed in her declaration. Instead, Ms. Charters' declaration reflects what she learned secondhand at executive meetings from Flagstar's Chief Information Security Officer ("CISO") and others that led Flagstar's data breach response.[6]

II. The Data Breach.

Flagstar contends that the data breach was a "garden-variety ransomware attack," confined to December 3–4, 2021. Mot. at 35, ECF No. 58, PageID.705. That is not true. The criminals' access to, and attacks on, Flagstar's infrastructure started before December 3, 2021, and persisted long after December 4, 2021.[7]

---

[3] Ex. 1, Transcript of Jennifer Charters' Deposition ("Charters Dep.") at 13:21–15:9; *see id.* at 91:22–92:7.
[4] *Id.* at 13:21–17:16; 27:8–14.
[5] *Id.* at 51:7–23.
[6] *See id.* at 32:11–15; 33:1–34:22; 39:3–41:15; 44:3–45:13; 52:14–54:4.
[7] *See id.* at 28:16–30:3.

On November 22, 2021, anonymous criminals infiltrated Flagstar's network using a contractor's stolen log-in credentials.[8] By November's end, Flagstar knew it had been breached.[9] It is not clear what action, if any, Flagstar took at this time to secure its network, and in any case, eleven days later, the criminals began mining Flagstar's network for data. By the end of the day on December 4, 2021, Flagstar contends that the threat actors had exfiltrated massive amounts of PII from Flagstar's network over a 48-hour period.[10] Ten days after exfiltration, and twenty-one days after the initial breach, Flagstar's systems were still under attack. On December 13, the criminals deployed ransomware, issued distributed denial of service attacks, and demanded [redacted] as a ransom for the stolen data.[11]

For the next several weeks, Tetra Defense, Inc. ("Tetra Defense") negotiated with the criminals on Flagstar's behalf.[12] Ms. Charters was not involved in the

---

[8] Ex. 2, Flagstar's Internal Talking Points Memorandum ("Talking Points Memo") (FLAG-DEC-00000053–55) at 54.

[9] Ex. 1, Charters Dep. 28:16–30:3.

[10] *Id.* Ms. Charters' testimony that data was exfiltrated "on December 3 and 4, 2021" is based on her memory of a "post-mortem" analysis performed by Flagstar's information security team and Kroll Associates, Inc. ("Kroll"). Kroll produced a report on this analysis in January or February of 2022, but Ms. Charters did not review the report before executing her declaration nearly a year and a half later, and Flagstar has refused to produce. *Id.* at 30:4–31:22; *see id.* at 16:9–17:11; Ex. 3, Oct. 23, 2023 Ltr, ¶ 12.

[11] Ex. 1, Charters Dep. 29:19–23; 47:15-48:2, 48:24-49:13; Ex. 4, Ransom Emails (FLAG-DEC-00000016–35) at 19. Ms. Charters did not personally receive any ransom demands. Ex. 1, Charters Dep. 34:23–35:16.

[12] Ex. 1, Charters Dep. 38:12–39:2; *see* Ex. 4, Ransom Emails at 19, 17. Ms. Charters was not involved in Flagstar's engagement of Tetra Defense and does not know who

ransom negotiations; she only knows what others, like the CISO, disclosed during executive meetings, and could not authenticate the ransom negotiation emails Flagstar produced (Ex. 4).[13] [redacted].[14]

Already facing blow-back for customer data leaked on the dark web during the Accellion data breach earlier that year, Flagstar sought [redacted].[15] Flagstar also sought deletion of the stolen data, [redacted].[16] Underscoring this point, [redacted]

---

at Tetra Defense was involved in the data breach response. Ex. 1, Charters Dep. 39:3–40:2; 41:12–15.

[13] *Id.* at 40:13–41:22; 45:24–47:2; 52:14–16.

[14] *See* Ex. 4, Ransom Emails at 32 ([redacted]); *Id.* at 22 ([redacted]); *Id.* at 24 ([redacted]).

[15] Ex. 4, Ransom Emails at 32 ([redacted]).

[16] *Id.* at 21 ([redacted]).

[redacted][17] Although negotiations were [redacted]

[redacted][18]

Ms. Charters learned of Flagstar's decision to pay the criminals from Flagstar's CEO during an executive meeting.[19] She was not involved in the decision to pay the ransom, nor was she privy to Flagstar's rationale for doing so.[20] When asked whether she agreed with the decision, Ms. Charters said that "it depends on the situation," but that "it certainly does not help to incent threat actors by paying them money to stop…harassing you."[21]

Not only does paying a ransom incentivize criminals, but law enforcement and data security experts uniformly agree that paying a ransom also "doesn't guarantee you or your organization will get any data back."[22] "[E]ven if you pay," the Federal Trade Commission warns, "you don't know if the cybercriminals will

---

[17] *Id.* at 29 ([redacted]).

[18] *Id.* at 28 ([redacted]). *See id.* at 26 ([redacted]); *Id.* at 27 ([redacted]); *Id.* at 28 ([redacted]).

[19] Ex. 1, Charters Dep. 52:14–16.

[20] *Id.* at 50:17–51:3; 53:3–6.

[21] *Id.* at 52:17–53:2.

[22] Ransomware, FBI.gov, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited March 1, 2024); CISA, Oct. 2023, StopRansomware Guide ("Paying ransom will not ensure…that your data will not be leaked.").

keep your data[.]"[23] William Hardin, Flagstar's purported cybersecurity and ransomware expert, confirmed that criminals can do whatever they want with stolen data.[24] Citing to what he coined as the "pirates code," Mr. Hardin explained that Flagstar would have to trust that the criminals wouldn't keep it,[25] that criminals can sell stolen data in piecemeal fashion under dark web aliases, and that Social Security numbers "can sell anywhere between ten cents to $3[.]"[26]

Nevertheless, on December 31, 2021, [redacted][28]

Flagstar's Motion states that the criminals followed through on that promise. Mot. at 20, ECF No. 58 PageID.690 ("On December 31, 2021, Flagstar paid $1 million, and Flagstar was given access to the server where the stolen data was stored, which Flagstar deleted"). They did not. [redacted]

[23] RansomWare, FTC, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/ransomware (last visited March 1, 2024).
[24] Ex. 5, Excerpts from the Transcript of William Hardin's Deposition ("Hardin Dep.") 285:2–4; 285:19–22; 286:20–287:11. Mr. Hardin had no personal involvement in the ransom negotiations. *See* Section II(B)(3).
[25] Ex. 5, Hardin Dep. 185:2–22; 239:2–17.
[26] *Id.* at 160:16–161:6; 161:13–24; 162:20–24.
[27] Ex. 4, Ransom Emails at 33 ([redacted]
[28] *Id.* ([redacted]).

[redacted].[29] Ms. Charters conceded that she does not know what the criminals did with Flagstar's stolen data during that seven-day gap between ransom payment and server access.[30]

When the criminals [redacted], they purportedly allowed Tetra Defense to access a "drive" using remote desktop protocol credentials.[31] Like the ransom negotiations, Ms. Charters was not involved in this effort.[32] Flagstar has produced no evidence establishing what data, if any, the criminals permitted Tetra Defense to access, or what Tetra Defense was able to do with it. Although [redacted].[33]

Ms. Charters, who was not involved in the ransom negotiations, nonetheless claimed in her declaration that Flagstar received "confirmation that there were no additional copies of the data[.]" Mot. at 30, ECF No. 58 PageID.700. At her deposition, however, she conceded that the only "confirmation" she knows about is [redacted]

[29] Ex. 4, Ransom Emails at 35 ([redacted]); *Id.* at 16 ([redacted]); Ex. 1, Charters Dep. 55:15–57:10.
[30] *Id.* at 57:7–13.
[31] *Id.* at 54:5–14.
[32] *Id.* at 55:8–14; 58:12–59:12.
[33] *See* Ex. 4, Ransom Emails at 34–35 ([redacted]).

[redacted][34] Those ransom emails, which Ms. Charters did not consult before executing her declaration,[35] reveal that [redacted].[36] Ms. Charters also confirmed she does not know whether the criminals destroyed the server.[37] The criminals also [redacted][38] Instead, [redacted].[40]

[34] Ex. 1, Charters Dep. 60:8–62:22.
[35] *See id.* at 45:24–46:21; 64:23–65:7.
[36] Ex. 4, Ransom Emails at 17 ([redacted]); *Id.* ([redacted]).
[37] Ex. 1, Charters Dep. 64:15–67:15 (explaining basis for declaration ¶ 7); *see also* Ex. 4, Ransom Emails at 17 ([redacted]).
[38] *See* Ex. 4, Ransom Emails at 32 ([redacted]).
[39] *See id.* at 29 ([redacted]).
[40] *Id.* at 17 ([redacted]); *Id.* at 17–18 ([redacted]); Ex. 1, Charters Dep. 64:2–14.

III. Flagstar's Post-Breach Response.

A. Flagstar's Investigation into What Data Was Stolen.

Flagstar relies on Ms. Charters to attest to what data the criminals stole. Yet Ms. Charters confirmed that she had no part in determining what data was stolen and did not oversee that work.[41] Flagstar's CISO, Information Security Team, and Data Analytics Group, along with Kroll, were responsible for that effort—together, they created a "master list" of individuals and data elements they believed were compromised in the breach.[42] Ms. Charters was not involved in creating that list,[43] and her declaration statements simply regurgitate what she saw when she reviewed excerpts from it.[44] Ms. Charters does not know whether Flagstar ever compared the data Tetra Defense purportedly deleted to the data Flagstar contends was stolen.[45] And although the criminals purportedly sent Flagstar a list of stolen files on December 13, 2021, Flagstar has failed to preserve that list.[46]

---

[41] *Id.* at 26:15–27:5; 68:6–8.
[42] *Id.* at 17:12–18:18; 19:18–23:21; 25:23–26:2; 86:24–90:13; 91:6-21.
[43] *Id.* at 12:24–13:8; 20:14-21:9; 26:15–27:5; 89:6–18; 91:6–21. Similarly, she was not involved in determining what Flagstar data was leaked on the dark web during the Accellion breach or who that breach impacted. *Id.* at 25:23–26:12; 94:20–98:22.
[44] *Id.* at 91:22–93:13.
[45] *Id.* at 59:13–60:6.
[46] Ex. 4, Ransom Emails at 19; Ex. 3, Oct. 23, 2023 Ltr, p. 3 ¶ 1 ("we have undertaken a search for such documents and have been unable to locate them.").

B. Flagstar's Investigation Into Who Has Access to the Data.

1. The Cyber Criminals' Identity.

The identities of the individuals with control of Flagstar's stolen data during the extended breach period, or thereafter, remain unclear. Ms. Charters testified that Flagstar's CISO told her that the criminals were part of a criminal group called "Shao,"[47] but Flagstar's counsel told Mr. Hardin at least part of the attack used ransomware associated with another criminal group, [redacted][48] While Mr. Hardin opines that [redacted] Mr. Hardin was not asked to render that opinion, and it raises further questions regarding who had access to Flagstar's data and what they did with it.[49]

2. Kroll's Dark Web Monitoring.

Ms. Charters also claims Kroll "conducted daily monitoring of the dark web" and "identified no evidence that the threat actor released any Flagstar data[.]" Doc. 58-3 ¶ 8, ECF No. 58-2 PageID.741–42. But her knowledge of Kroll's dark web

---

[47] Ex. 1, Charters Dep. 33:1–20.

[48] Ex. 6, Jan. 12, 2024 Email ("The statement in paragraph 10 of Mr. Hardin's declaration derives from facts provided by Flagstar's counsel."); *see* Ex. 5, Hardin Dep. 194:16–22.

[49] *Id.* at 87:17–89:17; *see also id.* at 184:12–185:22; 189:3-190:3; 202:22–205:22; 210:11–211:13. Mr. Hardin also stated, based on [redacted], that he believes Shao would have followed the "pirates code" and not posted stolen data on the dark web; he did not provide any support for this speculation. *See id.* at 91:4–94:22; 185:10–189:2.

monitoring, and the results, is limited to others told her.[50] Ms. Charters had no role interfacing with Kroll, does not know how Kroll performed its dark web search, and does not know how Kroll presented its findings to Flagstar—she was not involved in that discussion.[51] In any case, Ms. Charters confirmed that Kroll did not begin its dark web monitoring until October 2022, ten months *after* the data breach occurred.[52]

3. CRA's Dark Web Monitoring.

Flagstar engaged William Hardin from CRA in October 2022, ten months after the breach, to research the presence of Flagstar's and Plaintiff Smith's data on the dark web.[53] Mr. Hardin stated his "number one objective" was "demonstrating that the [stolen] information had been deleted."[54]

At his deposition, Mr. Hardin confirmed that CRA only searched the dark web for two weeks, from October 28, 2022 to November 14, 2022, and that CRA's search would, thus, only find data that was available on whatever sections of the dark web CRA searched on those dates.[55]

---

[50] Ex. 1, Charters Dep. 84:19–86:23.
[51] *Id.*
[52] *Id.* at 84:11–18.
[53] Ex. 5, Hardin Dep. 51:18–52:7. Mr. Hardin did not search for any other Plaintiff. *Id.* at 264:13–22.
[54] *Id.* at 238:21–239:1.
[55] *Id.* at 115:14–116:4; 120:13–121:13.

Mr. Hardin also admitted that CRA only searched [redacted] dark web sites, a small "fraction" of an "unlimited," "unknown," number of sites on the dark web.[56] Exhibit B to Mr. Hardin's Declaration [redacted].[57] Mr. Hardin confirmed that during the time of the data breach, the cyber criminals could have been active on any number of marketplaces that he did not search.[58] Likewise, Exhibit C to Mr. Hardin's Declaration lists the [redacted] "shame sites" CRA reviewed in its analysis.[59] Mr. Hardin did not expect Flagstar's data to be posted on any of these sites, because Flagstar paid a ransom.[60] Even so, Mr. Hardin confirmed that shame sites may exist today, and at the time of the data breach, that CRA did not search.[61] In fact, [redacted].[62] Ultimately, Mr. Hardin testified that he does not know, and it would be impossible to quantify, how many dark web sites CRA did *not* review, particularly because they are "constantly changing."[63]

---

[56] *See* ECF No. 58-3 PageID.771–77. Ex. 5, Hardin Dep. 54:16–55:12; 74:19–24. The dark web does not have a search engine; users must have access to each site's particular web address, or "onion link." *Id.* at 52:8–19.
[57] *Id.* at 58:6–10; 73:10–75:20; 179:16–21.
[58] *Id.* at 179:10–21.
[59] *Id.* at 60:13–22; 63:23–64:3; 65:19–66:16. "Shame sites" are used by criminals to shame victims who have not paid a ransom. *Id.* at 70:1–9.
[60] *Id.* at 69:8–70:9; 115:1–5.
[61] *Id.* at 66:17–67:10; *see also id.* at 61:8–16; 63:7–16.
[62] *Id.* at 276:9–22.
[63] *See id.* at 258:2–259:21.

Finally, Mr. Hardin confirmed that he did not know what data was stolen in the data breach.[64] Instead, [redacted]".[65] Mr. Hardin claims CRA [redacted] but did not retain those communications.[66] Mr. Hardin confirmed that CRA did not keep written documentation on this analysis.[67]

ARGUMENT

I. PLAINTIFFS HAVE ARTICLE III STANDING.

To establish standing under Article III, Plaintiffs must show (1) an injury-in-fact, (2) that is "fairly traceable" to Flagstar's conduct, and (3) that a court can redress. *Spokeo v. Robins*, 578 U.S. 330, 338 (2016). Under Rule 12(b)(1), defendants may challenge the pleading itself (facial attack) or the factual existence of subject matter jurisdiction (factual attack). *Cartwright v. Garner*, 751 F.3d 752, 759 (6th Cir. 2014). A facial attack questions whether the plaintiff has alleged a basis for subject matter jurisdiction, and the court assumes the truth of the allegations. *Id.* In a factual attack, the defendant asserts that Plaintiffs' jurisdictional allegations are

[64] *Id.* at 162:6–11.
[65] *Id.* at 100:23–107:1; Ex. 6, Jan. 12, 2024 Email.
[66] Ex. 5, Hardin Dep. 108:1–109:13; Ex. 6, Jan. 12, 2024 Email ("Any communications [were] not retained.").
[67] Ex. 5, Hardin Dep. 112:6–17.

"not true" and must "demonstrate a lack of genuine issue of material fact as to the jurisdictional question[.]" *In re Blackbaud, Inc., Customer Data Breach Litig.*, 2021 WL 2718439, at *4 (D.S.C. July 1, 2021); *Kal Kan Foods, Inc. v. Iams Co.*, 197 F. Supp. 2d 1061, 1067 (S.D. Ohio 2002).

Flagstar disputes that Plaintiffs plausibly allege injury-in-fact or traceability (the facial attack) and claims extrinsic facts demonstrate Plaintiffs' injuries are not traceable to Flagstar's conduct (the factual attack). Neither challenge has merit.

A. Plaintiffs Plausibly Allege Injury in Fact.

To fulfill the injury requirement, Plaintiffs must allege they suffered "an invasion of a legally protected interest" that is "concrete and particularized," and "actual or imminent." *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016).[68] An injury-in-fact exists where there is a "substantial risk" that harm will occur that prompts Plaintiffs to "reasonably incur costs to mitigate or avoid the harm[.]" *Id.* (citing *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 414 n.5 (2013)).

Plaintiffs allege several forms of injury resulting from the data breach, including actual fraud and identity theft, the imminent and continuing substantial risk thereof, time and money spent on self-protection after the breach, loss in value of their PII, anxiety and loss of privacy, and loss of the benefit of their bargain with

[68] Although *Galaria* is an unpublished decision, its analysis on standing is persuasive. *See Lochridge v. Quality Temp. Servs., Inc.*, 2023 WL 4303577, at *4 (E.D. Mich. June 30, 2023).

Flagstar. *See* CAC ¶¶ 6–19, 77–86, ECF No. 52 PageID.547–556, 582–586. These allegations of concrete injuries plausibly establish Article III standing, as numerous courts have held in data breach cases, including cases following the Supreme Court's holding *TransUnion*. *See, e.g.*, *Galaria*, 663 F. App'x at 388; *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1206 (S.D. Fla. 2022); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459 (D. Md. 2020); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1315–18 (N.D. Ga. 2019); *In re Experian Data Breach Litig.*, 2016 WL 7973595, at *3–5 (C.D. Cal. Dec. 29, 2016).

1. Several Plaintiffs Have Suffered Actual Fraud, and All Plaintiffs Face an Imminent Risk of Fraud.

Cyber criminals infiltrated Flagstar's network and stole Plaintiffs' PII—including their Social Security numbers, account and loan numbers, and names—to engage in identity theft, financial fraud, or to sell it to other criminals. CAC ¶¶ 77–79, ECF No. 52 PageID.582. Multiple Plaintiffs received notice that their PII is on the dark web, and several Plaintiffs have suffered actual and attempted identity theft and fraud. *Id.* ¶¶ 8, 15–17, PageID.582, 548, 552–554.[69] Because of Flagstar's failure

[69] Plaintiffs' allegations of misuse underscore the imminent risk of harm to all Plaintiffs. *See, e.g., In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig. ("OPM")*, 928 F.3d 42, 59 (D.C. Cir. 2019). So do Plaintiffs' allegations of attempted fraud and increase in phishing communications. Flagstar's argument to the contrary relies on inapposite cases. *See* Section I(C) *infra*. Mot. at 27–28, ECF No. 58 PageID.697–98 (citing *Cooper v. Bonobos, Inc.*, 2022 WL 170622, at *4

to secure Plaintiffs' PII, all Plaintiffs now suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of their PII. *Id.* ¶¶ 6–19, 77–86, PageID.547–556, 582–586. *Galaria* instructs that these are cognizable Article II injuries. 663 F. App'x at 388; *see Marriott*, 2020 WL 869241, at *6 (plaintiffs should not "have to wait until they…suffer identity theft to bring their claims.").[70]

Flagstar contends that *Galaria* is no longer valid after the Supreme Court's decision in *TransUnion*. Mot. at 31, ECF No. 58 PageID.701. Multiple courts have rejected that argument. *Lochridge*, 2023 WL 4303577, at *4 ("Defendant argues that, following the Supreme Court's decision in *TransUnion*, the holding of *Galaria* is no longer valid. The court disagrees.").[71]

(S.D.N.Y. Jan. 19, 2022) (finding plaintiff failed to plead a risk of future identity theft where only partial credit card information was leaked) and *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) (finding plaintiff could not "plausibly face a threat of future fraud" for theft of her physical credit card where plaintiff canceled it before any fraud was committed; distinguishing *Galaria*)).

[70] *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690–94 (7th Cir. 2015) (finding there was an "objectively reasonable likelihood" that injury would occur to customers whose credit card information was stolen where some had already experienced fraudulent charges).

[71] *Batts v. Gannett Co.*, 2023 WL 3143695, at *3 (E.D. Mich. Mar. 30, 2023) (Kumar, D.J.) ("*TransUnion* merely reiterates the canons of *Spokeo*"); *Brickman v. Maximus, Inc.*, 2022 WL 16836186, at *4 (S.D. Ohio May 2, 2022) (finding standing under *Galaria*). *See Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 156 (3d Cir. 2022) ("a plaintiff suing for damages can satisfy concreteness as long as [the plaintiff] alleges that the exposure to that substantial risk [of identity theft or fraud] caused additional, currently felt concrete harms" such as "emotional distress" or money spent "on mitigation measures."). *See also Bohnak v. Marsh & McLennan Companies, Inc.*, 79

Flagstar also contends that Plaintiffs have not established a substantial risk of harm and "cannot plausibly allege that the risk of identity theft has materialized[.]" Mot. at 31-32, 35, ECF No. 58 PageID.701-2, 705. But instead of analyzing Plaintiffs' allegations under *Galaria*, Flagstar simply ignores them, asserting that "Flagstar paid the ransom, so the cyber criminals do not even possess the data at issue," and the data breach was a "garden-variety ransomware attack," whose "primary purpose" was "extortion, not identity theft[.]" Mot. at 35–36, ECF No. 58 PageID.705-6.[72] These statements are disputed (*see* Section I(D)–(E), *supra*), contradict Plaintiffs' allegations, and are not appropriate in a facial attack. CAC ¶¶ 6–19, 77–80, ECF No. 52 PageID.547–556, 582–83; *see Cartwright*, 751 F.3d at 759; *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 969 (7th Cir. 2016) ("[The argument that] any fraudulent charges cannot be attributed to the data breach…is a theory of defense that [defendant] will be entitled to pursue at the merits phase."); *Marriott*, 2020 WL 869241, at *13.

Further, none of Flagstar's cases considers the facts of this case. *In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022), *report and recommendation adopted*, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022)

F.4th 276, 286 (2d Cir. 2023) (same); *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 373 (1st Cir. 2023) (same).

[72] *Shepherd v. Cancer & Hematology Centers of W. Michigan, P.C.*, 2023 WL 4056342 (W.D. Mich. Feb. 28, 2023) (factual attack on standing involving data breach that did not impact plaintiffs' personal information).

(no allegations of misuse and plaintiffs conceded the purpose of the attack was extortion); *In re SuperValu, Inc.*, 870 F.3d 763, 770 (8th Cir. 2017) (stolen data did not include PII); *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 994 (W.D. Okla. 2021) (no allegations that plaintiff "or any other class member" was victim of fraud); *Quintero v. Metro Santurce, Inc.*, 2021 WL 5855752, at *2, 6 (D.P.R. Dec. 9, 2021) (no allegations of misuse or exfiltration, distinguishing *Galaria*).

2. Plaintiffs' Time and Expense to Mitigate Fraud are Cognizable Injuries.

Each Plaintiff has taken mitigating actions resulting in concrete injuries, spending time and effort responding to the imminent risks of fraud, like monitoring their accounts and freezing their credit. CAC ¶¶ 6–19, ECF No. 52 PageID.547-556. As the Sixth Circuit recognized in *Galaria*, allegations of "a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury[.]" 663 F. App'x at 388; *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262–63 (11th Cir. 2021); *Marriott*, 2020 WL 869241, at *37.

As the Sixth Circuit explained in *Galaria*, Plaintiffs' mitigation efforts are not an attempt to manufacture standing because Plaintiffs' data "has already been

stolen." 663 F. App'x at 388.[73] Indeed, Flagstar recommended taking these very steps. CAC ¶¶ 38, 43–45, ECF No. 52 PageID.564, 566–67; *Galaria*, 663 F. App'x at 388 ("there is no need for speculation" particularly where, as here, the defendant "recommended taking these steps."); *Remijas*, 794 F. 3d at 694 ("It is unlikely that [defendant offered credit monitoring] because the risk is so ephemeral that it can safely be disregarded."). It would be "unreasonable to expect Plaintiffs to wait for actual misuse" before "taking steps to ensure their own personal and financial security," a fact that Flagstar's offer of credit monitoring does not change. *See Galaria*, 663 F. App'x at 388; *see* CAC ¶ 38, ECF No. 52 PageID.564 (alleging Flagstar's credit monitoring offer is inadequate to compensate Plaintiffs).[74]

3. The Lost Value of Plaintiffs' PII is a Cognizable Injury.

Plaintiffs allege their PII (including their Social Security numbers and names) had significant value not only to Plaintiffs, but to Flagstar, who uses Plaintiffs' PII to increase its profits, and that value is diminished now that it is in the hands of criminals who can, and have, used it to commit fraud. *See* CAC ¶¶ 7, 23, 79, 82,

[73] *Garland v. Orlans, PC*, cited by Flagstar, is therefore inapposite. *See* 999 F.3d 432, 441 (6th Cir. 2021) (explaining that anxiety experienced by plaintiff related to a default was self-inflicted).

[74] *Dearing v. Magellan Health Inc.* lends no support for Flagstar's position. 2020 WL 7041059, at *3 (D. Ariz. Sept. 3, 2020) ("Here, Plaintiff's PII and PHI did not appear to be deliberately targeted, and there is no evidence the information was even stolen").

ECF No. 52 PageID.547, 557, 582, 584. This loss in value is a cognizable harm. *See Marriott*, 440 F. Supp. 3d at 460–461 ("[T]he growing trend across courts that have considered this issue is to recognize the lost property value of [personally identifying] information.") (collecting cases).[75]

Marriott also explained that Plaintiffs do not need to allege they intended to sell their PII, noting the "common sense" conclusion that PII has value "in our increasingly digital economy." 440 F. Supp. 3d at 462.; *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (plaintiffs are not required to plead that there is a market for their PII and that they intended to sell it). Flagstar's reliance on disputed and unsupported factual allegations does not change this result.

4. Plaintiffs' Loss of Privacy is a Cognizable Injury.

Plaintiffs' emotional distress, anxiety, and increased concerns for the loss of their privacy are also concrete injuries. CAC ¶¶ 6–19, ECF No. 52 PageID.547–556; *Gerber v. Herskovitz*, 14 F.4th 500, 507 (6th Cir. 2021) (holding that emotional harm satisfies Article III standing after *TransUnion*); *Hopper v. Credit Associates, LLC*, 2022 WL 943182, at *4 (S.D. Ohio Mar. 29, 2022) ("[c]ourts have traditionally

[75] *See also Stamat v. Grandizio Wilkins Little & Matthews, LLP*, 2022 WL 3919685, at *7 (D. Md. Aug. 31, 2022) (explaining that "economic loss in value could be recognizable as a concrete injury…the misuse of PII can damage its value") (distinguishing *Galaria*).

provided an avenue of relief for alleged violations of privacy" in finding injury-in-fact requirement satisfied); *Pratt v. KSE Sportsman Media, Inc.*, 586 F. Supp. 3d 666, 676 (E.D. Mich. 2022). Flagstar's citation to disputed material facts, and inapposite cases and does not persuade otherwise.[76]

5. Plaintiffs' Loss of the Benefit of the Bargain with Flagstar is a Cognizable Injury.

Plaintiffs allege they overpaid for Flagstar's services, which is also a cognizable harm. *See* CAC ¶¶ 7, 84, ECF No. 52 PageID.547–48, 584–85. Neither of Flagstar's cases is on point.[77] Many courts have concluded that similar allegations state a cognizable injury in fact. *See Marriott*, 440 F. Supp. 3d at 462–66 (similar allegations were "enough" to adequately allege injury).[78]

[76] *Duqum v. Scottrade, Inc.*, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016), aff'd sub nom. *Kuhns v. Scottrade, Inc.*, 868 F.3d 711 (8th Cir. 2017) (no allegations of identity theft or fraud); *Darnell v. Wyndham Cap. Mortg., Inc.*, 2021 WL 1124792, at *5–6 (W.D.N.C. Mar. 24, 2021) (no allegations that PII was target of phishing scheme); *Patterson v. Med. Rev. Inst. of Am., LLC*, 2022 WL 2267673, at *2 (N.D. Cal. June 23, 2022) ("undisputed evidence" showed criminals returned data).

[77] *In re: Cmty. Health Sys., Inc.*, 2016 WL 4732630, at *7 (N.D. Ala. Sept. 12, 2016) (plaintiffs did not allege they paid a premium for data protection or received information about data protection other than a HIPAA notice); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 26–27 (D.D.C. 2014) (plaintiffs did not allege data was viewed or misused after thief broke into a car and stole encrypted backup data tapes).

[78] *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 909 (8th Cir. 2016) (same); *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 992, 995–96 (N.D. Cal. 2016) (same); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018) (same).

B. Plaintiffs Plausibly Allege Standing to Seek Injunctive Relief.

Plaintiffs allege an immediate threat of future injury because Flagstar's inadequate security measures continue to put Plaintiffs' PII, still in Flagstar's possession, in jeopardy. CAC ¶¶ 85, 196, ECF No. 52 PageID.585, 620. This breach was Flagstar's second major data breach in a single year, and Flagstar remains a prime target for cyberattacks. *Id.* ¶¶ 46–60, ECF No. 52 PageID.568–574. These allegations support Plaintiffs' standing to pursue injunctive relief. *Finesse Express, LLC v. Total Quality Logistics, LLC*, 2021 WL 1192521, *5 (S.D. Ohio Mar. 30, 2021) (allegations that defendant, who retained plaintiffs' confidential information had its inadequate post-breach security measures was sufficient for injunctive relief standing); *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1252 (D. Colo. 2018) (same).

None of Flagstar's factually distinct cases from the Second, Third, and Fourth Circuits counsels otherwise. *See, e.g., Galaria*, 663 F. App'x at 389–90 ("*Reilly* is not on point where, as here, Plaintiffs allege an 'identifiable taking'—the intentional theft of their data.") (citing 664 F.3d 38, 44–46 (3d Cir. 2011)); *Graham v. Universal Health Serv., Inc.*, 539 F. Supp. 3d 481, 487 (E.D. Pa. 2021) (explaining that cases from the Sixth, Seventh, Ninth, and Tenth Circuits, including *Galaria*, which found "standing based on increased risk of harm…may indeed have a more realistic view of the impact of data thefts on consumers").

C. Plaintiffs Plausibly Allege Injuries Fairly Traceable to Flagstar.

To survive a facial attack to traceability, plaintiffs in a data breach case need only allege that the defendant was a "plausible source of [their] personal information." *Blackbaud,* 2021 WL 2718439, at *8–9 (this burden is "relatively modest"). Plaintiffs have done so. Because of Flagstar's lax security, criminals stole Plaintiffs' PII from Flagstar; Flagstar contacted Plaintiffs about the breach and instructed them on mitigation steps; and Plaintiffs experienced fraud and other harms.[79] CAC ¶¶ 6–19, 77–86, ECF No. 52 PageID.547–556, 582–586. These allegations satisfy Article III traceability. *Galaria*, 663 F. App'x. at 390 (citing consistent holdings from the Eleventh, Seventh, and Ninth Circuits); *Remijas*, 794 F.3d at 696 (defendant's admission that data might have been exposed and that it contacted victims to warn of the risk "raise[d] the plaintiffs' right to relief above the speculative level.").

Plaintiffs also plausibly link their harm to Flagstar's conduct. Plaintiffs allege criminals stole their PII, including Social Security numbers, account and loan numbers, and names, and that criminals can commit (and have committed) fraud

[79] Plaintiffs' allegations of unwanted, post-breach phishing communications also support standing. *See, e.g., Mednax*, 603 F. Supp. 3d at 1205–06; *Desue v. 20/20 Eye Care Network, Inc.*, 2022 WL 796367, *3 (S.D. Fla. Mar. 15, 2022); *In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *7 (S.D.N.Y. Aug. 4, 2021). Flagstar's inapposite case cite does not dictate otherwise. *Supra*, Section I(A)(1) (distinguishing *Legg*).

with that information. CAC ¶¶ 33, 77, 79, 162, ECF No. 52 PageID.562, 582, 610. Plaintiffs allege their injuries were a result of the data breach. *Id.* ¶¶ 8, 10–12, 15–18, ECF No. 52 PageID.548–51, 552–55. These allegations, which neither of Flagstar's cases addresses, are enough.[80] *See SuperValu*, 870 F.3d at 772 (courts "presume that general allegations embrace those specific facts that are necessary to support a link between [plaintiff's] fraudulent charge and the data breach."); *Blackbaud,* 2021 WL 2718439, at *9; *Mednax*, 603 F. Supp. 3d at 1206 (stolen data "could very well have been enough to aid [in the commission of identity theft]"); *Experian*, 2016 WL 7973595, at *3; *cf. In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018) (stolen data "still gave the hackers means to commit fraud" even where social security numbers were not stolen).

Finally, the fact that some Plaintiffs may have had their data exposed in other data breaches "does nothing to negate the plaintiffs' standing to sue[.]" *Remijas*, 794 F.3d at 696 ("[i]t is certainly plausible for pleading purposes that their injuries are 'fairly traceable' to the data breach"). That rings particularly true where, as here, Plaintiffs' PII may have been exposed in the earlier Accellion breach, also involving

[80] *McCombs v. Delta Grp. Elecs., Inc.*, 2023 WL 3934666, *5 (D.N.M. June 9, 2023) (plaintiff failed "to allege that any of the compromised PII—whether hers or that of the proposed class—has been misused"); *In re: Cmty. Health Sys.*, 2016 WL 4732630, at *12 (no allegation that breach "involved specific financial information"). Plaintiff Nasrallah alleges unauthorized accounts and filed tax returns— the very injuries that *Cmty Health Sys.* found traceable. *Id.* at *12.

Flagstar. *See Lewert*, 819 F.3d at 969 ("Merely identifying potential alternative causes does not defeat standing"). Flagstar "does not get a free pass on this basis." *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 651 (N.D. Cal. 2020).

D. Flagstar's Factual Attack is a Premature Merits Attack.

Flagstar invites error by asking this Court to resolve factual disputes essential to the merits of Plaintiffs' claims. A district court should engage in a factual inquiry regarding the complaint's allegations "only when the facts necessary to sustain jurisdiction do not implicate the merits of the plaintiff's claim." *Gentek Bldg. Prod., Inc. v. Sherwin-Williams Co.*, 491 F.3d 320, 330–31 (6th Cir. 2007). If a factual attack "implicates an element" of a claim the court should "find that jurisdiction exists" and consider the objection "a direct attack on the merits of the plaintiff's claim." *Id.* In the data breach context, courts routinely reject similar factual attacks at the pleading stage. *See Blackbaud,* 2021 WL 2718439, at *7–8.

In a nearly identical factual attack, Blackbaud argued plaintiffs' injuries were not traceable to the data breach because an external cybersecurity firm concluded there was "'no evidence' that [p]laintiffs' PII was on the dark web or being marketed for sale." *Id.* at *7. Rejecting the factual attack, the Court explained that defendant's motion was "essentially, an indirect attack on Plaintiffs' alleged factual merits[,]" because the facts necessary to "prove jurisdiction" overlapped with facts relevant to the causation element of plaintiffs' claims. *Id.* at *8.

So too, here. Flagstar's factual challenge to traceability disputes that there is a "causal connection" between Plaintiffs' injuries and Flagstar's actions. Mot. at 29–30, ECF No. 58 PageID.700. Because causation is an element of Plaintiffs' tort and statutory claims, Flagstar's challenge is an indirect, if not direct, attack on the merits. *See id.* at 59, PageID.715. Plaintiffs must be permitted to fully develop the record before the Court can resolve the issues. *See* ECF No. 65 PageID.877 (declining to engage in further "merits discovery").

Accordingly, Flagstar's factual attack must be denied. *See, e.g., Allgood v. PaperlessPay Corp.*, 2022 WL 846070, at *5 (M.D. Fla. Mar. 22, 2022) (denying factual attack, finding defendants' argument that plaintiffs could not have suffered fraud or identity theft from a data breach was a direct attack on the merits); *Mednax*, 603 F. Supp. 3d at 1207 (same); *MSP Recovery LLC v. Progressive Select Ins. Co.*, 2015 WL 10457208, at *2 (S.D. Fla. May 18, 2015) (denying factual attack because court needed to consider "the entire factual record" at summary judgment); *Brown v. Allied Comm'ns Corp.*, 2020 WL 868207, at *4 (S.D. Ohio Feb. 21, 2020) (denying factual attack implicating merits of plaintiff's claim).

E. Flagstar's Factual Attack Raises Material, Disputed Facts.

If the Court determines it should reach the merits of these factual issues now, the proper standard is that applied at summary judgment: "the moving party in a factual challenge is required to demonstrate a lack of genuine issue of material fact

as to the jurisdictional question, either through the submission of evidence or by making a 'showing' that Plaintiff cannot establish the necessary facts." *Kal Kan Foods*, 197 F. Supp. 2d at 1067 (citing *Armbruster v. Quinn*, 711 F.2d 1332, 1335 (6th Cir. 1983)). Here, Flagstar has offered no competent evidence establishing what data was stolen and when, who stole it, and what those actors might have done with it during, and for months following, the breach.[81]

First, Flagstar contends that it "deleted the exfiltrated data from the cyber criminal's server and received confirmation that there were no additional copies of the data." Mot. at 30, ECF No. 58 PageID.700. Ms. Charters was not involved in the data exfiltration or ransom negotiations and has no relevant first-hand knowledge on those subjects. *Supra* SOF Sections I–II.

Second, Flagstar contends that the stolen data was "*never* available on the dark web." Mot. at 30, ECF No. 58 PageID.700. But Flagstar has submitted no evidence that the stolen data was not misused or made available on the dark web for the ten months after the data breach, because neither Kroll nor CRA conducted dark web monitoring until October 2022. *Supra*, SOF Section IIII(2)–(3).[82] Likewise,

[81] As set forth throughout this response, Ms. Charters' declaration does not meet the standard of Rule 54(c)(4), because it is not based on her personal knowledge. The Court should therefore disregard the declaration in considering the application of a Rule 56 standard to these issues.

[82] This revelation also calls into question Flagstar's assurances to consumers in June 2022, that it "identified no evidence" of misuse. CAC ¶ 40, ECF No. 52 PageID.565.

neither source establishes the absence of the stolen data on the dark web *after* October 2022. Ms. Charters has no relevant, first-hand knowledge of Kroll's dark web monitoring or its results; she only knows what others at Flagstar told her. *Supra*, SOF Section III(2). And CRA only searched [redacted] dark web sites for a two-week period. CRA did not have access to the stolen data, and instead, only [redacted]. *Supra*, SOF Section III(B)(3).

Third, Flagstar contends several Plaintiffs' PII was "definitely *not* compromised" in the data breach. Mot. at 30, ECF No. 58 PageID.700. But Ms. Charters has no personal knowledge on this topic; she based her testimony on "excerpts" of a list that she did not create. *Supra*, SOF Section III(A).

Finally, Flagstar acknowledges that at least seven Plaintiffs' Flagstar-related PII *is* on the dark web. Although Flagstar attributes this to the Accellion breach Flagstar experienced earlier in 2021, Ms. Charters has no personal knowledge on this topic, either. *Supra*, SOF Section II. In any case, whether Plaintiffs have had PII exposed in other breaches is irrelevant to standing. *See* Section I(C), *supra*.

Thus, the Court should not resolve the factual issues raised by Flagstar based on its declarations. *See Bischoff v. Osceola County*, 222 F.3d 874, 875 (11th Cir. 2000) (district court erred by resolving "central factual disputes and ma[king] witness credibility choices on issues material to standing just by relying on its

reading of warring affidavits"); *Lawrence v. Dunbar*, 919 F.2d 1525, 1530 (11th Cir. 1990) (vacating district court's dismissal under 12(b)(1) where affiant "lacked personal knowledge of many of the key events in this case").

II. PLAINTIFFS SUFFICIENTLY ALLEGE THEIR COMMON LAW CLAIMS.

A. Choice of Law.

Michigan's choice-of-law rules "pose a fact-intensive inquiry that additional discovery would help to resolve." *Scott Eisenberg of CRS Capstone P'nrs, LLC v. Alterna Cap. Sols., LLC*, 2023 WL 348334, at *3 (E.D. Mich. Jan. 20, 2023). Here, several jurisdictions "have a stake in this litigation." *Id.*; CAC ¶¶ 6–19, ECF No. 52 PageID.547–556 (alleging Plaintiffs are citizens of California, Colorado, Florida, Indiana, Michigan, Missouri, and Washington). Because a factual record is needed to adequately address the choice of law analysis, Flagstar's motion should be denied to the extent it relies on material differences in the potentially applicable laws at issue. *See Foisie v. Worcester Polytechnic Inst.*, 967 F.3d 27, 41–44 (1st Cir. 2020) (reversing choice-of-law determination at pleading stage); *Wise v. Zwicker & Assocs., P.C.*, 780 F.3d 710, 718–19 (6th Cir. 2015) (same); *In re OnStar Cont. Litig.*, 600 F. Supp. 2d 861, 865 (E.D. Mich. 2009) (holding choice-of-law analysis would be premature without limited discovery). Thus, Plaintiffs' opposition responds to Flagstar's arguments premised on Michigan law, but also addresses, where relevant, other potentially applicable laws.

B. Plaintiffs State a Claim for Negligence.

1. Plaintiffs Plausibly Allege Flagstar Breached a Duty.

Plaintiffs plausibly allege Flagstar breached its duty of care by, among other things, failing to comply with state and federal law and industry standards governing the protection of PII, and concealing, for over six months, that Plaintiffs' PII was stolen. *See, e.g.,* CAC ¶¶ 34–46, 53, 61–76, ECF No. 52 PageID.562–569, 574–581; *In re GEICO Customer Data Breach Litig.*, 2023 WL 4778646, at *15 (E.D.N.Y. July 21, 2023) (plaintiffs plausibly alleged defendant breached "by failing to adopt, implement, and maintain fair, reasonable, or adequate security measures" despite foreseeable risk); *Hummel v. Teijin Automotive Technologies, Inc.*, 2023 WL 6149059, at *7–8 (E.D. Mich. Sept. 20, 2023); *GE*, 2021 WL 3406374, at *8.

Flagstar has not publicly disclosed "the manner in which [Flagstar's] systems were breached," nor the "specific measures" it took to protect Plaintiffs' PII. *See* Mot. at 41, ECF No. 58 PageID.711; CAC ¶¶ 35–39, 76, ECF No. 52 PageID.562–65, 581. Plaintiffs could not plead those facts without discovery. *See Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1220 (11th Cir. 2023) ("A plaintiff may know only what the company has disclosed in its notice of a data breach."); *Flores-Mendez v. Zoosk, Inc.*, 2021 WL 308543, at *4 (N.D. Cal., Jan. 30, 2021) ("[an] ordinary consumer, however, has no clue what internet companies' security steps are" thus the court could "reasonably infer[] at the pleadings stage" that security measures

were inadequate); *Mackey v. Belden, Inc.*, 2021 WL 3363174, at *6 (E.D. Mo. Aug. 3, 2021) (plaintiff "cannot be expected to have access to detailed information regarding [defendant's] cybersecurity" at pleading stage). Further Plaintiffs do not seek to hold Flagstar liable "for the fact of the data breach alone," and *In re Waste Mgmt.* is therefore inapposite. 2022 WL 561734, at *7 (S.D.N.Y. Feb. 24, 2022).

2. Plaintiffs Allege Plausible Injuries.

All Plaintiffs allege plausible injuries. The two cases Flagstar cites are inapposite. In *Doe v. Henry Ford Health Sys.*, no data was stolen or accessed for misuse after patient records were inadvertently made temporarily available online. 308 Mich. App. 592, 601 n.6 (2014) (comparing its opinion to cases involving "a data breach when there has been no evidence of identity theft[.]"). So too for *Rakyta v. Munson Healthcare*. 2021 WL 4808339, at *3 (Mich. Ct. App. Oct. 14, 2021) ("plaintiff did not allege that she *or any other potential class member*" was a victim of identity theft) (emphasis added). Here, Plaintiffs allege data was actually stolen and posted on the dark web. *See* CAC ¶¶ 6, 11, 18, 41–42, 78, ECF No. 52 PageID.547, 550–51, 554–55, 565–66, 582. These allegations render Plaintiffs' injuries plausible. *See Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889 (11th Cir. 2023) (fact that hackers posted stolen PII on the dark web establishes a "present

injury" and a "substantial risk of future injury").[83]

Explained further in Section I(A), Plaintiffs allege several injuries arising from Flagstar's negligence, including mitigation time and expenses and increased risk of fraud. Accepted as true, these cognizable injuries support negligence claims in various states. *See In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 402–03 (E.D. Va. 2020) (imminent threat of identity theft is a plausible injury under California and Florida negligence law); *Marriott*, 440 F. Supp. 3d at 494 ("the losses incurred to mitigate the harms are adequately pled damages in addition to being an injury-in-fact" for Florida negligence claim); *Huynh*, 508 F. Supp. 3d at 650 (time and money spent on credit monitoring are plausible injuries

[83] Plaintiffs also state a claim for negligence *per se* (Count 2) based on Flagstar's violations of Section 5 of the Federal Trade Commission (FTC) Act and the Gramm-Leach-Bliley Act (GLBA). *See* CAC ¶¶ 61–76, 118–131, ECF No. 52 PageID.574–581, 600–603. Courts routinely conclude that violation of Section 5 creates negligence *per se* liability. *See, e.g., Marriott*, 440 F. Supp. 3d at 479; *Equifax*, 362 F. Supp. 3d at 1327–28. Violation of the GLBA's Safeguards Rule may also give rise to negligence *per se* liability. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 371 F. Supp. 3d 1150, 1174 (N.D. Ga. 2019) ("the Safeguards Rule provides an ascertainable standard of conduct permitting it to serve as the basis for a negligence per se claim"). Flagstar's argument for dismissal conflates the state-law claim asserted and the federal doctrine of implied rights of action. *See Lowe v. Gen. Motors Corp.*, 624 F.2d 1373, 1379 (5th Cir. 1980) ("that the law which evidences negligence is Federal while the negligence action itself is brought under State common law does not mean that the state law claim metamorphoses into a private right of action under Federal regulatory law.").

under California negligence law).[84] For these same reasons, Plaintiffs have plausibly alleged damages not only for their negligence claims, but their breach of confidence and other torts claims as well. *See* Mot. at 46 n.8, ECF No. 58 PageID.716.

3. Plaintiffs Plausibly Allege Causation.

For the reasons stated in Section I(C), Plaintiffs plead both a logical and temporal relationship between the Data Breach and the injuries they experienced. *See* CAC ¶¶ 6–19, 77–86, ECF No. 52 PageID.547–556, 582–86; *see, e.g.*, *McKenzie v. Allconnect, Inc.,* 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019) (finding causation for negligence claim where, as here, "there is no dispute that an unauthorized data release occurred in this case that resulted in Plaintiffs' personal information being released to unknown third-parties"); *Experian*, 2016 WL 7973595, at *3 ("Defendants also argue that since the stolen PII didn't include credit card numbers, the complaint also fails for not alleging how this data breach could have caused his fraudulent credit card charges. This argument isn't supported by any case law that requires such specific allegations of causation at a 12(b)(6) stage and is unconvincing to the Court."); *Equifax*, 362 F. Supp. 3d at 1319 (whether "prior breaches caused" plaintiffs' injuries is "purely a dispute of fact not appropriate for resolution at this stage of the litigation").

[84] *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *8 (M.D. Fla. Jan. 27, 2020) (plaintiffs stated a Florida negligence claim where some Plaintiffs alleged fraud).

C. Plaintiffs State a Claim for Breach of Confidence.

"A breach of confidence involves 'the unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship.'" *Eickenroth v. Roosen, Varchetti & Olivier, PLLC*, 2021 WL 1224912, at *4 (E.D. Mich. Mar. 31, 2021). Courts have recognized this as a viable claim against banks and other entities outside of the trade-secret context.[85] *See McGuire v. Shubert*, 722 A.2d 1087, 1091 (Pa. Super. Ct. 1998) (recognizing banker's duty not to disclose customer's information); *Milohnich v. First Nat. Bank of Miami Springs*, 224 So. 2d 759, 762 (Fla. Ct. App. 1969) (same). Plaintiffs plausibly allege this claim here, because Flagstar breached their confidence and caused them to suffer damages by knowingly allowing the unauthorized disclosure of their PII due to inadequate security measures. *See, e.g., Cap. One*, 488 F. Supp. 3d at 409 (upholding similar claim where defendant "allowed a known vulnerability to persist on its systems which…exposed the bank's customers' data to potential breach"); *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019) (explaining the harm underlying a breach of confidence "transpires when a third party gains

[85] *See*, *e.g.*, *State Farm Mut. Auto. Ins. Co. v. Elite Health Centers, Inc.*, 2019 WL 2576360, at *3 (E.D. Mich. June 24, 2019) (breach of confidence in an attorney-client relationship); *Richard v. Detroit Tr. Co.*, 257 N.W. 725, 727 (Mich. 1934) (breach of confidence can arise out of promise to marry). Other states also recognize breach of confidence claims. *Cap. One*, 488 F. Supp. 3d at 409 (Florida and California); *Pac. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1205, 1212 (E.D. Wash. 2003) (Washington).

unauthorized access to a plaintiff's personal information," as is the case here).[86]

D. Plaintiffs State a Claim for Breach of Privacy.

Plaintiffs allege that Flagstar intruded upon their private affairs by permitting the unauthorized disclosure of their PII. *Dickson v. Direct Energy, LP*, 69 F.4th 338, 345 (6th Cir. 2023) ("The intrusion-upon-seclusion tort…safeguards the right to be secluded from and undisturbed by the public."). Plaintiffs further allege that Flagstar did so knowingly, by failing to secure their PII despite knowing the risks caused by its inadequate security measures and that it was a likely target of attacks seeking this kind of information. CAC ¶¶ 45, 54, ECF No. 52 PageID.567, 570–71. Both Flagstar's conduct in facilitating this intrusion and the intrusion itself are highly offensive to a reasonable person. *Id.* at ¶¶ 161–163, PageID.610–11. Courts routinely recognize that these facts give rise to an actionable tort of intrusion upon seclusion. *See*, *e.g.*, *McKenzie*, 369 F. Supp. 3d at 819; *Curry v. Schletter Inc*., 2018 WL 1472485, at *4 (W.D.N.C. Mar. 26, 2018); *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 926 (S.D. Cal. 2020).

[86] Flagstar's argument that a breach of confidence claim requires the intentional or voluntary disclosure of information is inapposite. Here, Plaintiffs allege Flagstar allowed a known vulnerability to exist unauthorized, all the while knowing it was a target for cybercriminals.

E. Plaintiffs State a Claim for Breach of Express Contract.

Plaintiffs allege Flagstar breached its express contractual promises to "protect your personal information from unauthorized access and use" by using "security measures that comply with federal law," including "computer safeguards and secured files and buildings[.]" CAC ¶¶ 165, 168, ECF No. 52 PageID.612. These promises limit the circumstances in which Flagstar is permitted to disclose customers' PII to third parties, which does not include a data breach. *See id.* ¶¶ 169–170, PageID.613.

Courts in the data breach context recognize that privacy notices contain enforceable promises. *See Marriott*, 440 F. Supp. 3d at 459 (rejecting *Dyer*, upholding contract claim based on privacy statements);[87] *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735 (W.D.N.Y. 2017) *on reconsideration*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018) (finding promises such as "We are committed to safeguarding your protected health information (PHI)" and "[A]ll computer systems that contain personal information have security protections" are enforceable); *Huong Hoang v. Amazon.com, Inc.*, 2012 WL 1088165, at *4 (W.D. Wash. Mar. 30, 2012) (upholding contract claim based on privacy policy).

[87] The language Flagstar cites from *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) is dicta and comes from a portion of the opinion dismissing breach of contract claims that the plaintiffs had already abandoned. *See* 334 F. Supp. 2d at 1199 n.2.

Plaintiffs also plausibly allege consideration—Flagstar benefited from maintaining and using Plaintiffs' PII, and Flagstar's promise to keep Plaintiffs' PII safe was given in exchange for that information. *See* CAC ¶¶ 7, 84, ECF No. 52 PageID.547–48, 584–85. Flagstar cites no cases suggesting otherwise. *Emergency Dep't Physicians P.C. v. United Healthcare, Inc.*, 507 F. Supp. 3d 814, 829 (E.D. Mich. 2020) (unrelated ERISA case); *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 52–53 (D. Ariz. 2021) (plaintiffs did not allege promises to act beyond HIPPA mandates).

Next, by alleging they provided their PII to Flagstar in exchange for Flagstar's services, Plaintiffs have plausibly alleged objective manifestations of mutual assent. *Rood v. Gen. Dynamics Corp.*, 507 N.W.2d 591, 598 (Mich. 1993) (recognizing that under Michigan law objective manifestations of assent are sufficient to form a contract); *Motor Co. v. Kahne*, 379 F. Supp. 2d 857, 869 (E.D. Mich. 2005);[88] *Marriott*, 440 F. Supp. 3d at 483–84 (rejecting argument that plaintiffs had to plead "they read, saw, or understood the Privacy Statements" under breach of contract theory, explaining that plaintiffs' acts of providing their personal information to Marriott "constitute objective manifestations of acceptance").

[88] The same standard for assent applies under other potentially applicable state laws. *See DeLeon v. Verizon Wireless, LLC*, 207 Cal. App. 4th 800, 813 (2012); *Kolodziej v. Mason*, 996 F. Supp. 2d 1237, 1246–47 (M.D. Fla. 2014); *City of Everett v. Sumstad's Estate*, 631 P.2d 366, 367 (Wash. 1981).

Further, it is well-settled that Michigan's statute of frauds does not pertain to agreements, like the one Plaintiffs allege, that are for an indefinite term. *See Chires v. Cumulus Broadcasting, LLC*, 543 F. Supp. 2d 712, 719 (E.D. Mich. 2008). Flagstar cites no case law suggesting otherwise and conflates federal law requirements with Flagstar's contractual obligations.

Plaintiffs also allege Flagstar breached its contractual promises by taking inadequate data security measures that violated industry standards, including Section 5 of the FTC Act and the GLBA's Safeguards Rule. CAC ¶¶ 71–76, 173, ECF No. 52 PageID.578–581, 613; *Capital One*, 488 F. Supp. 3d at 411 (plaintiffs adequately alleged defendant breached its contractual promise to use security measures that comply with federal law).[89]

Finally, Plaintiffs have alleged damages from Flagstar's breach of contract. CAC ¶¶ 6–19, 174, 182, ECF No. 52 PageID.547–556, 613–14, 616–17; *see Hummel*, 2023 WL 6149059, at *11–12. *Doe* and *Rakyta* are inapposite. Section II(B)(2). Even if Plaintiffs did not suffer actual damages, Michigan law infers nominal damages from a breach of contract, which are sufficient to state a cause of

[89] *Kuhns v. Scottrade, Inc.*, does not support dismissal on this basis. *See Hall v. Centerspace, LP*, 2023 WL 3435100, at *6 (D. Minn. May 12, 2023) (rejecting similar argument based on *Kuhns*, explaining "[e]lsewhere in the Complaint," plaintiff "specifically asserts" that defendant "failed to comply with industry standards, failed to adequately train employees…failed to follow several FTC guidelines…and delayed prompt notice upon discovery of data breach") (citing *Kuhns*).

action under Michigan law.[90] *See Broad-Ocean Techs., LLC v. Lei*, 649 F. Supp. 3d 584, 596 (E.D. Mich. 2023) (Lawson, J.); *Ford Motor Co. v. Versata Software, Inc.*, 2018 WL 4282740, at *5 (E.D. Mich. Sept. 7, 2018).

F. Plaintiffs State a Claim for Breach of Implied Contract.

Implied contracts arise from the conduct of the parties. *Hummel*, 2023 WL 6149059, at *8. By taking possession of Plaintiffs' PII, Plaintiffs allege Flagstar created an obligation to provide adequate data security. CAC ¶¶ 176–179, ECF No. 52 PageID.615. Flagstar breached this obligation by failing to do so, and by disclosing Plaintiffs' PII to unauthorized third parties. *Id.* ¶ 181, PageID.616. In data breach litigation, Courts routinely find these allegations support a breach of implied contract claims. *See Marriott*, 440 F. Supp. 3d at 459; *Rudolph v. Hudson's Bay Co.*, 2019 WL 2023713, at *11 (S.D.N.Y. May 7, 2019) (collecting cases); *Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d 739, 750–751 (S.D.N.Y. 2017) (finding representations in privacy policy could support implicit promise); *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015) *aff'd sub nom.* 739 F. App'x 91 (3d Cir. 2018) (concluding defendants "through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to

[90] Plaintiffs are entitled to nominal damages for all their common law claims. *See Taylor v. City of Saginaw*, 620 F. Supp. 3d 655, 671 (E.D. Mich. 2022) ("At common law…'every injury imports a damage,' even if that damage is nominal." (quoting *Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 799 (2021)).

safeguard [plaintiff's] PII"). As this district has recognized, it is "difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of [PII] would not imply the recipient's assent to protect the information sufficiently." *Hummel*, 2023 WL 6149059, at *11 (citing *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016)).

Plaintiffs also plausibly allege mutual assent. *See* CAC ¶¶ 176–80, ECF No. 52 PageID.615–16; *Hummel*, 2023 WL 6149059 at *10–11 ("courts around the country have found the existence of mutual assent even in the absence of clear definitive terms outlining the specific measures a party would take to protect PII"); *Lochridge*, 2023 WL 4303577, at * 7 (allegation that the defendant required the plaintiff to provide his information to utilize their services was sufficient to plead mutual assent). Neither of Flagstar's cases is analogous.[91] Flagstar's remaining arguments mirror those raised against the breach of express contract claim and fail for the same reasons. Section II(E), *supra*.

G. Plaintiffs State a Claim for Unjust Enrichment.

Plaintiffs allege Flagstar was unjustly enriched by taking, retaining, and using Plaintiffs' PII for its own gain without expending sufficient resources to adequately

[91] *Supervalu*, 870 F.3d at 771 n.6 (cursory analysis of breach of contract claims in the standing context, explaining "a plaintiff who has produced facts indicating that it was a party to a breached contract has a judicially cognizable interest for standing purposes"); *Cmty. Bank of Trenton v. Schnuck Mkts. Inc.*, 2017 WL 1551330, at *5 (S.D. Ill. May 1, 2017) (case on behalf of banks).

protect it. CAC ¶¶ 134–148, ECF No. 52 PageID.604–06. Courts in data breaches recognize the value of such data, both to the businesses that use it to profit, and the consumers who rely on its integrity to engage in transactions. *See Marriott*, 440 F. Supp. 3d at 460–61 (collecting cases); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) (plaintiffs' personal information was valuable to defendant, who used it for targeted advertising).

Further, any benefit conferred on Flagstar would be unjust if retained. Plaintiffs allege that part of the money they paid Flagstar should have covered the costs of properly securing their PII. CAC ¶ 139 ECF No. 52 PageID.605. By failing to fund adequate security, Flagstar retained that money. These are plausible allegations of unjust enrichment. *See, e.g., In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 538 (M.D. Pa. 2021) (plaintiff stated claim for unjust enrichment where they alleged they paid for data security); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1317 (11th Cir. 2012) (premiums used in part to provide data protection conferred unrecompensed benefit).

H. Plaintiffs State a Claim for Declaratory Judgment.

For the same reasons cited in Section I(B), *supra*, Plaintiffs have plausibly alleged a continuing risk supporting their entitlement to bring a declaratory judgment claim. *See Finesse Express*, 2021 WL 1192521, *8–9 (rejecting similar argument to Flagstar's and finding declaratory judgment claim adequately pled where plaintiffs'

claims would not otherwise clarify defendant's prospective obligations to safeguard plaintiffs' information); *In re: Home Depot, Inc. Customer Data Sec. Breach Litig.*, 2016 WL 2897520, *4 (N.D. Ga. May 18, 2016) (denying motion to dismiss claim for declaratory and injunctive relief where plaintiffs alleged defendant's security measures continued to be inadequate). Flagstar cites only to *Lochridge*, but that case is inapposite. 2023 WL 4303577, at *8 ("[plaintiff has not alleged any facts tending to show that…there is a substantial risk that [a second data breach] will occur.").

III. PLAINTIFFS SUFFICIENTLY ALLEGE THEIR STATUTORY CLAIMS.

A. Plaintiffs' CCRA and WDBDL Claims Are Sufficiently Pled.[92]

The California and Washington Plaintiffs allege plausible claims under the California Customer Records Act ("CCRA") and Washington Data Breach Disclosure Law ("WDBDL"). First, Plaintiffs plausibly allege that Flagstar's delayed notice was unreasonable and caused them harm—Flagstar failed to disclose the data breach until June 2022, despite learning of the breach in at least December 2021 and conducting an extensive investigation thereafter. CAC ¶ 33–45, ECF No. 52 PageID.562–67. Whether this delay was reasonable is a material question of fact. Further, Plaintiffs allege Flagstar's unreasonable, six-month delay prevented them

[92] Plaintiffs withdraw their claim for violation of the Colorado Security Breach Notification Act (Count 13).

from taking steps to protect against fraud and identity theft sooner; indeed, all Plaintiffs allege they sought to mitigate damages after they learned of the breach. *Id.* ¶¶ 33–45; 8–9, 19, PageID.562–67, 548–49, 555–56. These facts are sufficient to establish incremental damages. *Mednax*, 603 F. Supp. 3d at 1219; *see Stasi*, 501 F. Supp. 3d at 925 (incremental harm satisfied by allegation that plaintiff could have taken steps to mitigate if notified sooner).

B. Plaintiffs State Claims Against Flagstar for Violation of State Statutes Prohibiting Unfair or Deceptive Conduct.

1. Plaintiffs Adequately Plead Unfair or Deceptive Conduct.

Plaintiffs allege that Flagstar violated the UCL, CLRA, IDCSA, CCPA, MCPA, WCPA by "engaging in unlawful, unfair, and deceptive business acts and practices," including "fail[ing] to implement and maintain reasonable security measures to protect Plaintiffs' and the [state] Subclass Members' PII from unauthorized disclosure[.]" CAC ¶¶ 214–15, 244–245, 259, 267–268, 285, ECF No. 52 PageID.624, 633–35, 639, 641–43, 646–48. They further allege that the failure to implement and maintain reasonable security measures was a violation of Section 5 of the FTC Act. *Id*. It is well-settled that when deceptive acts or unfair practices are premised on violation of Section 5 of the FTC Act, Rule 9(b) does not apply. *F.T.C. v. Communidyne, Inc.*, 1993 WL 558754, at *2 (N.D. Ill. Dec. 3, 1993); *Equifax*, 362

F. Supp. 3d at 1335; *F.T.C. v. Hornbeam Special Situations, LLC*, 308 F. Supp. 3d 1280, 1286–87 (N.D. Ga. 2018).

But even if Rule 9(b) applied, Plaintiffs' allegations are sufficient because they state the who, what, where, and when of the wrongful conduct; Flagstar cites no authority suggesting otherwise. First, Plaintiffs identify the "who"—Flagstar—inappropriately retained and stored Plaintiffs' data in an insecure manner. CAC ¶¶ 5, 23, 32, 53, 60, ECF No. 52 PageID.547–48, 557, 562, 569, 574. Second, Plaintiffs plead specific affirmative misrepresentations in which Flagstar stated it would protect Plaintiffs' PII. *Id.* ¶¶ 1, 24, 26, 29–31, PageID.545, 558, 559, 560–61. Other data breach cases have upheld essentially identical claims. *See Experian*, 2016 WL 7973595, at *5; *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1166 (D. Minn. 2014). Third, Plaintiffs detail specific material omissions or deceptive acts. CAC ¶¶ 53, 63, 71, 75–76, ECF No. 52 PageID.569–70, 575, 578, 581. Plaintiffs plausibly allege Flagstar had a duty to disclose material facts regarding its inadequate security practices to safeguard Plaintiffs' PII. *See, e.g.,* CAC ¶¶ 228, 236, 259, ECF No. 52 PageID.630–32, 639; *Gordon*, 344 F. Supp. 3d at 1251; *Marriott*, 440 F. Supp. 3d at 489.[93]

[93] For these same reasons, Plaintiff Worton has also plausibly alleged an "incurable deceptive act" under the IDCSA. *Bray*, 2018 WL 11226516, at *6 (plaintiff alleged an "incurable act" where defendant "misrepresented that it would adequately protect customer information and failed to inform customers that it did not maintain adequate data protection systems").

Fourth, Plaintiffs provide the "when and where" for the above statements, as Flagstar's data security policies were in effect prior to and after the Data Breach. CAC ¶¶ 167–169, ECF No. 52 PageID.612–613. Finally, contrary to Flagstar's suggestion, Plaintiffs pled reliance by stating they would have acted differently had they known the truth about Flagstar's security practices. *See* CAC ¶¶ 7, 84, ECF No. 52 PageID.547–48, 584–85. In data breach cases, these allegations satisfy the limited reliance requirements that exist in some consumer protection statutes. *See*, *e.g.*, *Friedman v. AARP, Inc.*, 855 F.3d 1047, 1055 (9th Cir. 2017) (for purposes of a UCL claim, a "misrepresentation is judged to be 'material' if a reasonable man would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question"); *Bray v. Gamestop Corp.*, 2018 WL 11226516, at *6 (D. Del. Mar. 16, 2018) (plaintiff stated IDCSA claim where he alleged he would not have made a purchase on GameStop's website if he knew it did not "maintain compliant data security systems.").

2. Plaintiffs Plausibly Allege Injuries and Causation.

First, as stated in Sections I(A) and (II)(B)(2), *supra*, Plaintiffs have alleged several forms of actual injury and damages typical of those in other data breach litigation sufficient to state their statutory claims under California, Washington, Indiana, Colorado, and Michigan's consumer protection statutes. *See* CAC ¶¶ 6–19;

77–86, ECF No. 52 PageID.547–556, 582–86; *Experian*, 2016 WL 7973595, at *5 ("a growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory'); *Equifax*, 362 F. Supp. 3d at 1335–38 (denying motion to dismiss most state consumer protection claims); *Target*, 66 F. Supp. 3d at 1166 (same); *Marriott*, 440 F. Supp. 3d at 492 & n.17 (benefit of the bargain losses cognizable under the UCL) (citing *Kwikset Corp. v. Super. Ct.*, 246 P.3d 877, 885–86 (Cal. 2011) (plaintiffs can establish UCL standing by paying by alleging they paid more than they actually valued the product)); *Anthem*, 162 F. Supp. 3d at 985 (benefit of the bargain losses and restitution are cognizable UCL injuries); *Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, *5 (C.D. Cal. June 15, 2015) (credit monitoring, identity theft protection losses are cognizable under the UCL); *Williams v. Foremost Ins. Co. Grand Rapids Michigan*, 2018 WL 1907523, at *5 (W.D. Wash. Apr. 23, 2018) (WCPA's injury requirement is met where "property interest or money is diminished because of the unlawful conduct…quantifiable monetary loss is not required").

Second, none of Flagstar's cases are on point. *See, e.g., In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767 (N.D. Cal. 2019) (dismissing UCL claim where plaintiffs did not pay "any money at all" to Facebook); *Aspen Am. Ins. Co. v. Blackbaud, Inc.*, 624 F. Supp. 3d 982 (N.D. Ind. 2022) (not involving IDCSA claims and no plaintiffs alleged their data was exposed); *Jackson*

v. Loews Hotels, Inc., 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (involving breach of less sensitive information: "name, phone number, email address (but not her email password), and mailing address").[94]

Finally, for the reasons stated in Sections I(C) and II(B)(3), *supra*, Plaintiffs have also plausibly connected their injuries to the data breach. *See Anthem*, 162 F. Supp. 3d at 987–88.

C. Plaintiffs State a California Consumer Privacy Act Claim.

Flagstar faults Plaintiffs for not detailing even more precisely how its breached security measures were inadequate. Explained in Section II(B)(1), Plaintiffs cannot plead what Flagstar has not disclosed. *Comerica Bank v. McDonald*, 2006 WL 3365599, at *2 (N.D. Cal. Nov. 17, 2006) (specificity is "relaxed" where facts lie exclusively within defendant's possession). Plaintiffs allege specific ways that Flagstar's security measures caused them harm; no more is required. *See* CAC ¶¶ 76–77, 193, ECF No. 52 PageID.38–39, 77; *see Mehta v. Robinhood Fin. LLC*, 2021 WL 6882377, at *8 (N.D. Cal. May 6, 2021) (permitting CCPA claim based on similar allegations); *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022) (same).[95]

[94] Plaintiffs also allege they have no adequate remedy at law. CAC ¶¶ 85, 147, 187, ECF No. 52 PageID.585, 606, 618.

[95] Unlike here, the plaintiffs in *Maag* and *Griffey* did not allege *any* facts to support their CCPA claim. 2021 WL 5605278, at *2; 562 F. Supp. 3d at 57.

Second, Plaintiffs plausibly allege entitlement to statutory damages. Flagstar acknowledges that Plaintiffs provided written notice of Flagstar's CCPA violations more than 30 days before they filed the Consolidated Complaint. Mot. at 55, ECF No. 58 PageID.725. Flagstar has been on notice of its deficiencies for over two years and does not claim that it intends to cure them if it receives a new notice letter, or that it is possible to do so. Yet Flagstar argues Plaintiffs did not satisfy the notice requirement, relying on an Arizona district court's unpublished interpretation of California law. *Id.* (citing *Griffey*, 2022 WL 1811165, at *6). But *Griffey* overlooked the purpose of giving 30 days' notice (to afford an opportunity to cure—which Plaintiffs here provided) and cites one case on express warranty law, not the CCPA.

California state and federal courts interpreting California consumer protection statutes with pre-suit notice provisions agree that a plaintiff need only provide notice prior to filing the operative complaint. *See, e.g.*, *Morgan v. AT&T Wireless Servs., Inc.*, 177 Cal. App. 4th 1235, 1261 (2009) (discussing the CLRA's similar notice requirement);[96] *Norman v. FCA US, LLC*, 2023 WL 6388926, at *18 (E.D. Mich. Sept. 30, 2023) (explaining *Morgan* "rebuk[ed] courts" that had adopted a strict approach to notice for "'fail[ing] to properly take into account the purpose of the

[96] *Griffey* did not address *Morgan*, and provided no reason to think the California Supreme Court would decide the CCPA notice issue differently. *See Allstate Ins. Co. v. Thrifty Rent-A-Car Sys., Inc.*, 249 F.3d 450, 454 (6th Cir. 2001). If anything, the Legislature indicated that notice under the CCPA is less important by providing that a CCPA violation may not be curable. Cal. Civ. Code § 1798.150(b).

notice requirement'"). Courts uphold similar claims where plaintiffs amended their complaint after sending notice. *See Gregorio v. Ford Motor Co.*, 522 F. Supp. 3d 264, 276 (E.D. Mich. 2021); *Goodman v. Intervet, Inc.*, 2023 WL 2368123, at *5 (D.N.J. Mar. 6, 2023). Thus, Plaintiffs complied with the CCPA's notice requirement. *See Kanfer v. Pharmacare US, Inc.*, 142 F. Supp. 3d 1091, 1107 (S.D. Cal. 2015).

CONCLUSION

For the foregoing reasons, Flagstar's Motion to Dismiss should be denied.

Dated: March 6, 2024

Respectfully submitted,

/s/ Norman E. Siegel
Norman E. Siegel, MO #44378
Jordan A. Kane, MO #71028
STUEVE SIEGEL HANSON LLP
460 Nichols Rd., Ste. 200
Kansas City, MO 64112
(816) 714-7100
siegel@stuevesiegel.com
kane@stuevesiegel.com

Interim Co-Lead Class Counsel

/s/ John Yanchunis
John Yanchunis
Patrick Barthle
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
Pbarthle@ForThePeople.com

Interim Co-Lead Class Counsel

/s/ David H. Fink
David H. Fink
Nathan J. Fink
Fink Bressack PLLC
38500 Woodward Avenue, Suite 350
Bloomfield Hills, Michigan 48304
(248) 971-2500
dfink@finkbressack.com

Interim Liaison Counsel